SecurPassword

Бестокенная двухфакторная аутентификация и самостоятельное сбрасывание пароля.

Токены больше не нужны!

SecurPassword позволяет пользователям использовать свои существующие персональные устройства, наряду с предварительно записанными секретными вопросами, для проведения аутентификации, сброса пароля домена в реальном времени.*

С ростом нашей зависимости от ИТ, количество и сложность паролей каждого пользователя становятся обременительными. При замене пароля ИТ-поддержка, как правило, получает огромное количество сообщений от разочарованных и запутавшихся пользователей, заблокированных из сети. SecurPassword предлагает революционный подход к организации безопасности пароля.

Особенности

Решение ***SecurPassword*** может предоставляться как программное решение на территории клиента или хоститься в рамках управляемой услуги:

- Пароли сбрасываются через бестокенную двухфакторную аутентификацию
- Мобильный телефон используется для подтверждения своей личности перед сбросом пароля
- Уведомление о сроке действия пароля доставляется через SMS
- Это сокращает отделу поддержки до 90% действий по сбросу паролей
- Автоматическое развертывание пользователей через групповое членство в протоколе LDAP
- Удаленный сброс пароля через браузер
- Местный сброс пароля в точке входа в систему
- Фиксированная ежегодная плата, которая вносится за каждого пользователя, без скрытых доплат.

Двухфакторная аутентификация одновременно с самопомощью сброс пароля

Пользователей все чаще просят поменять свои пароли на более сложные. Это часто приводит к путанице или потере паролей и создает нагрузку справочную ИТ-отдела: чем больше организация, тем больше такая нагрузка.

Забытый пароль означает не только необходимость помощи для сброса данных пользователя, он также включает в себя безошибочную идентификацию пользователя. Благодаря процессу двухфакторной аутентификации с элементом самообслуживания пользователь принимает на себя ответственность за процесс и может самостоятельно решить проблемы, связанные с паролем, без привлечения службы поддержки.

Пользователи имеют возможность подключиться к автоматизированной веб-странице самопомощи, или через свою Графическую систему опознания и отождествления, и сбросить свой пароль через процесс двухфакторной аутентификации, который сочетает в себе предварительно записанный секретный вопрос наряду с их предпочитаемым устройством аутентификации. В качестве альтернативы предварительно записанному секретному вопросу, пользователю может быть предложено ввести такую информацию, как свой идентификационный номер сотрудника или другие данные, хранящиеся в существующем хранилище пользователя.

После завершения проверки личности, пользователю будет предложено ввести новый пароль, который соответствует правилам, установленным в организации. После этого ***SecurPassword*** сбрасывает пароль в режиме реального времени.

Многие организации получают быструю отдачу от своих инвестиций в ***SecurPassword***, при этом в некоторых компаниях запросы в службу поддержки о сбросе пароля сокращаются на 100%.

*У пользователя может быть только один профиль, который может быть активирован только на одном устройстве в один период времени.

Authenticate your way

SecurEnvoy является первопроходцем в области бестокенной двухфакторной аутентификации. Наши инновационные решения обеспечивают удобную, безопасную аутентификацию, которая в разы дешевле, чем аутентификация с использованием маркеров, и применяется по всему миру тысячами клиентов.

Контроль получает пользователь

Мы считаем, что для аутентификации пользователи должны иметь возможность выбрать любое персональное устройство в качестве своего токена, будь то мобильный телефон, планшет, ноутбук или даже рабочий телефон. Пользователи должны иметь возможность легко переносить свои идентификационные данные с одного устройства на другое, не оставляя персональных сведений на устаревших носителях.

Мир без аппаратных ключей безопасности

Аппаратные ключи безопасности, появившиеся более 30 лет назад, препятствуют массовому распространению двухфакторной аутентификации, так как они дороги при развертывании и запуске и нелегко масштабироваться. Пользователи не могут носить с собой отдельные аппаратные ключи для каждого вида деятельности — офиса, банка и т.д. Становится очевидным, что использование существующего личного устройства, такого как мобильный телефон, является решением проблемы.

Будучи изобретателями бестокенной аутентификации, мы намерены продолжать разрабатывать инновационные решения, основанные на персональных устройствах пользователей и решать проблемы, мешающие распространению таких решений, такие как задержки SMS, отсутствие телефонного сигнала или проблемы синхронизации.

Элегантная простота

Мы считаем, что процесс входа в систему должны быть как можно более простым, что тысячи пользователей могут быть включены в работу нажатием одной кнопки, при этом сохраняя высокий уровень безопасности. Наши концепции усиливают существующую инфраструктуру, например, Active Directory в качестве центральной базы данных, и создают простые и элегантные решения.

SecurEnvoy plc I info@SecurEnvoy.com I www.SecurEnvoy.com